What is claimed is:

1. An architecture for confirming the identity of a message sender on a remote services system, comprising:

a communications module operable to transmit a message;

a cryptographic module in said communication module for providing encryption of a data stream in said message;

a mid-level manager operating in conjunction with said communications module for controlling the flow of messages in said remote services system and for verifying the identity of a sender by comparing first and second data identities in said data stream.

2. The architecture according to claim 2, said first data identify comprising data in a network software layer, said second data identity comprising data in an application software layer.

3. The architecture according to claim 2, said cryptographic module employing secure socket layer encryption.

4. The architecture according to claim 2, said mid-level manager controlling data flow between a customer proxy and an applications server.

5. The architecture according to claim 4, wherein said mid-level manager is a customer mid-level manager.

6. The architecture according to claim 4, wherein said mid-level manager is an aggregation mid-level manager.

7. The architecture according to claim 2, wherein transmission of said message is conditioned on HTTP.

8. The architecture according to claim 2, wherein transmission of said message is conditioned on email protocol.

9. A method of confirming the identity of a message sender on a remote services system, comprising:

obtaining a first identity related to a message, said first identity being obtained from a first software layer in said remote services system;

obtaining a second identity related to the sender of a messages, said second identity being obtained from a second software layer in said remote services system; and

comparing said first identity with said second identity to verify the identity of the sender of said message.

10. The method according to claim 9, said first software layer being the network software layer, said second software layer being the application software layer.

11. The method according to claim 10, further comprising encrypting said message and said identities in an encryption module in said remote services system.

12. The method according to claim 11, said encryption of said data and said identities being performed in accordance with secure socket layer protocol.

13. The method according to claim 12, said message being transmitted in said system using HTTP protocol.

14. The method according to claim 12, said message being transmitted in said system using email protocol.

15. A method of confirming the identity of a message sender on a remote services system, comprising:

transmitting a message using a communications module of said remote services system;

encrypting a data stream in said message using an encryption module in said communications module; and

controlling the flow of said message in said remote services system using a mid-level manager, said mid-level manager verifying the identity of a sender by comparing first and second data identities in said data stream.

16. The method according to claim 15, said first identity comprising encrypted data in a network software layer of said remote services system, said second identity comprising encrypted data in an application software layer of said remote services system.

17. The method according to claim 15, said encryption module using secure socket layer protocol to encrypt said data stream.

18. The method according to claim 17, said mid-level manager controlling data flow between a customer proxy and an applications server.

19. The method according to claim 15, wherein said mid-level manager is a customer mid-level manager.

20. The method according to claim 15, wherein said mid-level manager is an aggregation mid-level manager.